**Project 3: DoS defender and Firewall Implementation using Mininet**

**PROJECT DOCUMENT**

**By- Vidya Nambiar**

**Krutika Kamilla**

**CONTENTS**

PROJECT SCOPE 1

INSTRUCTION TO RUN THE PROGRAM 1

PROGRAM OUTPUT 3

# 

# PROJECT SCOPE

This project adds DoS (denial of service) defender and firewall functionality into POX controller.

There are three hosts H1, H2 and H3 in our topology. As a firewall, it prevents packet flow between hosts H1 and H2 but allows packet flows between H1 and H3 and between H2 and H3. As a DoS defender, it protects host H3 from other hosts, which try to attack it flooding it with many packets to make H3 unavailable to legitimate users. DoS preventer can be used to protect any server from attack from malicious users.

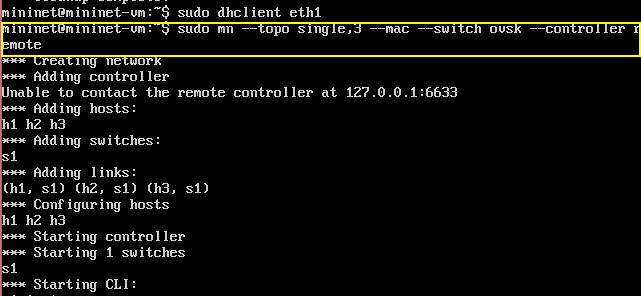
# INSTRUCTIONS TO RUN THE PROGRAM

1. Run “sudo mn –c” and restart Mininet to make sure that everything is "clean" and using the faster kernel switch. From your Mininet console:

$ sudo mn –c

2. Create the topology using the below command:

$ sudo mn --topo single,3 --mac --switch ovsk --controller remote



3. Then download the POX code from the [POX repository on github](https://github.com/noxrepo/pox) into your VM in /mininet folder:

$ git clone <http://github.com/noxrepo/pox>

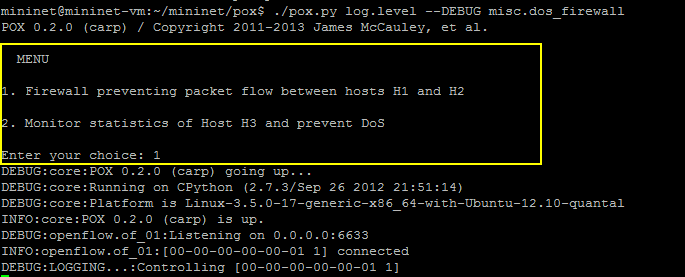
4. Go to the /mininet/pox/pox/misc folder and paste the python code provided “dos\_firewall.py”

$ cd mininet/pox/pox/misc

5.Go back to the /pox folder where the pox.py file is present and run the following command:

$ ./pox.py log.level --DEBUG misc.dos\_firewall

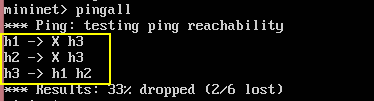
6. Make a selection from the given two options-



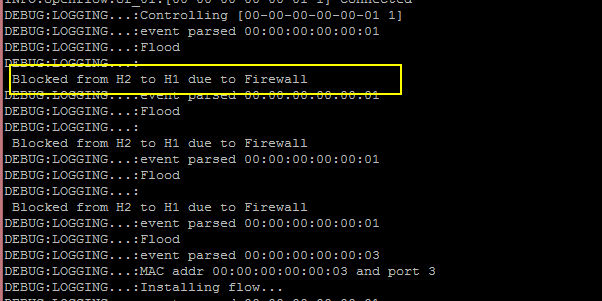
On selecting option 1 and hitting the enter key following things are to be done:

* 1. Start sending the packets to all hosts from all hosts through ping in the mininet console:

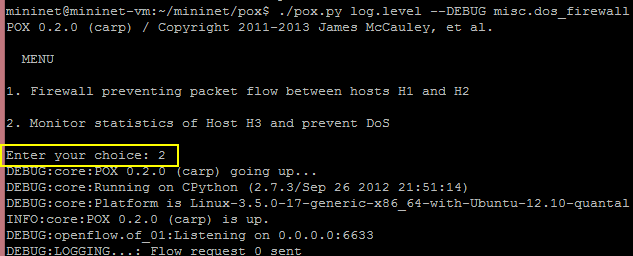
Mininet> pingall



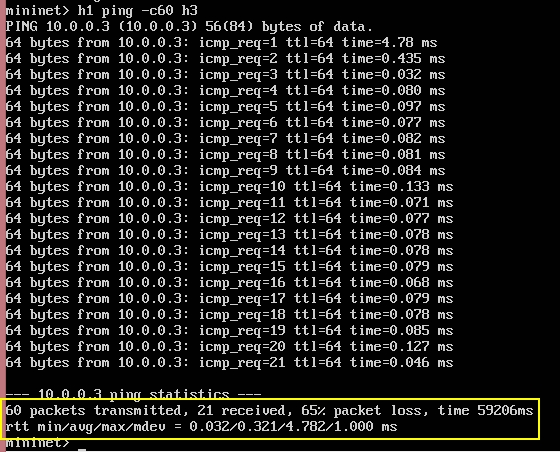
The output is as expected as the packets from h1🡪h2 and h2🡪h1 are blocked and all other hosts are able to ping eachother.



On selecting option 2 and hitting the enter key the following things are to be done:

a. 

After hitting enter key, start a ping of 60 packets to H3 from H1.



Then after the count of the number of packets exceeds a certain large number (inorder to test, we have taken the count as >2002 bytes to detect DoS but in real time scenario the count will be very large.)

As shown in the above output, 65% of the packets are lost as when the count >2002 bytes, all the succeeding packets are dropped as a way of preventing DoS attack from happening. This way we prevent Dos attack from happening.

Below is the output showing the prevention:

